IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

1. (Currently amended) An encryption device comprising XOR means and nonlinear transform means, said encryption device further comprising:

a random number generator ~~means~~ for generating a random number h, where h is an integer between zero and q-1;

q sets of fixed values, where q is equal to two, wherein equations, $FM_{0,h} = C_h$ XOR $L1_0(FMin)$, $C_h = c_{h,15}c_{h,1}...c_{h,0}$, and $D_h = d_{h,15}d_{h,14}...d_{h,0}$, are satisfied, where $FM_{i,h}$ is the i-th fixed value of the h-th set of said q sets of fixed values, where i is an integer and j is an integer,

q sets of fixed values, wherein equations, ($c_{0,j}$ XOR $c_{1,j}$) = (0101...01)2 or (1010...10)2 and ($d_{0,j}$ XOR $d_{1,j}$) = (0101...01)2 or (1010...10)2 are satisfied, a fixed table before masking is defined as S[x], and i-th masked fixed table is defined as $S_j[x \text{ XOR } c_{i,j}] \text{ XOR } d_{i,j}$ for the j-th fixed value,

~~q is an integer;~~linear transform means $L1_i(x)$, and linear transform means $L2_i(x)$, wherein the linear transform means $L1_i(x)$, the nonlinear transform means with the masked fixed table $S_j[x]$ and the linear transform means $L2_i(x)$ operate in i-th one of rounds; and

a first selector for selecting one fixed value of the h-th set of said q sets of fixed values in response to the random ~~number;~~ number h;

said XOR means XORing an input thereto with an XOR of a key with said selected fixed value.

2. (Cancelled)

3. (Currently amended) The encryption device according to claim 1, further comprising:

an encrypting unit comprising said first XOR means and said nonlinear transform means;

second XOR means for XORing an input to said encryption device with a fixed value selected in response to the random number h; and

third XOR means for XORing an output from said encrypting unit with the fixed value selected in response to the random number h.

4. (Currently amended) An encryption device comprising XOR means and nonlinear transform means, said encryption device further comprising:

a random number generator ~~means~~ for generating a random number h, where h is an integer between zero and q-1;

q sets of fixed values~~sets of masked fixed tables~~, where q is an ~~integer; and~~integer equal to three or more, wherein equations, $FM_{j,h} = C_h$ XOR L1i(L2i-1(Dh)) for i≥1, $C_h = c_{h,15}c_{h,14}...c_{h,0}$, and $D_h = d_{h,15}d_{h,14}...d_{h,0}$, where i is an integer and j is an integer,

q sets of fixed values, wherein equations, $(c_{0,j}$ XOR $c_{1,j}) = (0101...01)2$ or $(1010...10)2$ and $(d_{0,j}$ XOR $d_{1,j}) = (0101...01)2$ or $(1010...10)2$ are satisfied, a fixed table before masking is defined as S[x], and i-th masked fixed table is defined as $S_j[x$ XOR $c_{i,j}]$ XOR $d_{i,j}$ for the j-th fixed value;

linear transform means $L1_j(x)$ and linear transform means $L2_j(x)$, wherein the linear transform means $L1_j(x)$, the nonlinear transform means with the masked fixed table $S_j[x]$ and the linear transform means $L2_j(x)$ operate in i-th one of rounds; and

a first selector for selecting one fixed value of the h-th set of said q sets of fixed values of said q sets of fixed tables in response to the random ~~number,~~number h,

said XOR means XORing an input thereto with an XOR of a key with said selected fixed value. ~~said nonlinear transform means nonlinearly transforming an input thereto in accordance with said selected set of fixed tables~~.

5-7. (Cancelled)

8. (Currently amended) ~~The~~An encryption device ~~according to claim 4, wherein~~comprising XOR means and nonlinear transform means, said encryption device further comprising:

a random number generator for generating a random number h, where h is an integer between zero and q-1;

q sets of fixed values, where q is an integer equal to three or more, wherein equations, $FM_{0,h} = C_h$ XOR $L1_0$ (FMin), $C_h = c_{h,15}c_{h,1}...c_{h,0}$, and $D_h = d_{h,15}d_{h,14}...d_{h,0}$, are satisfied, where $FM_{j,h}$ is the i-th fixed value of the h-th set of said q sets of fixed values, where i is an integer and j is an integer,

~~an equation,~~q sets of fixed values, wherein equations, $(c_{0,j}$ XOR $c_{1,j}) \vee (c_{1,j}$ XOR $c_{2,j}) \vee ... \vee (cq_{-2,j}$ XOR $cq_{-1,j}) = (111...11)2$ and ~~$(d_{0,j}$ XOR $d_{1,j}) Ú (d_{1,j}$ XOR $d_{2,j}) Ú ... Ú (dq_{-2,j}$ XOR $dq_{-2,j}) =$~~

~~(11111111)2, is~~ $(d_{0,j}$ XOR $d_{1,j}) \vee (d_{1,j}$ XOR $d_{2,j}) \vee \ldots \vee (dq_{-2,j}$ XOR $dq_{-1,j}) = (111\ldots11)2$ are satisfied, ~~where~~ a fixed table before masking is defined as S[x], and i-th masked fixed table is defined as $S_j[x$ XOR $c_{i,j}]$ XOR $d_{i,j}$ for the j-th fixed value;

linear transform means $L1_j(x)$ and linear transform means $L2_j(x)$, wherein the linear transform means $L1_j(x)$, the nonlinear transform means with the masked fixed table $S_j[x]$ and the linear transform means $L2_j(x)$ operate in i-th one of rounds; and

a first selector for selecting one fixed value of the h-th set of said q sets of fixed values in response to the random number h,

said XOR means XORing an input thereto with an XOR of a key with said selected fixed value

~~a j-th masked table is defined as $S_j[x$ XOR $c_{i,j}]$ XOR $d_{i,j}$ (j = 0, 1, ... 15).~~

9. (Currently amended) The encryption device according to claim 4, said nonlinear transform means being Subbyte means;

the linear transform means $L1_j(x)$ ~~said encryption device further~~ comprising means for shifting an input, and the linear transform means $L2_j(x)$ comprising means for mixedcolumning an input.

10-15 (Cancelled)

16. (Currently amended) An encryption device comprising a random number generator ~~means~~ for generating a random number h, where h is an integer between zero and q-1, and a first plurality of encrypting rounds, wherein

i-th one ~~each~~ of said plurality of encrypting rounds comprises nonlinear transform means for nonlinearly transforming an input thereto, and XOR means for XORing a first input thereto with a second input thereto, for that round, where i is an integer;

the second input to said XOR means is coupled to an output of said nonlinear transform means; and

said nonlinear transform means comprises:

q sets of fixed values, where q is equal to two, wherein equations, $FM_{0,h} = C_h$ XOR $L1_0$ (FMin), $C_h = c_{h,15}c_{h,1}\ldots c_{h,0}$, and $D_h = d_{h,15}d_{h,14}\ldots d_{h,0}$, are satisfied, where $FM_{j,h}$ is the i-th fixed value of the h-th set of said q sets of fixed values, where ~~q is an integer;~~ j is an integer,

q sets of fixed values, wherein equations, $(c_{0,j}$ XOR $c_{1,j}) = (0101\ldots01)2$ or $(1010\ldots10)2$ and $(d_{0,j}$ XOR $d_{1,j}) = (0101\ldots01)2$ or $(1010\ldots10)2$ are satisfied, a fixed table before masking is

defined as S[x] and i-th masked fixed table is defined as $S_i[x \text{ XOR } c_{i,j}] \text{ XOR } d_{i,j}$ for the j-th fixed value;

a selector for selecting one of said q sets of fixed values in response to the random number h; ~~and~~

further XOR means for XORing an input thereto with an XOR of a key with said selected fixed ~~value.~~value;

linear transform means $L1_i(x)$;

a plurality of nonlinear transform means for nonlinearly transforming an input in accordance with a fixed table;

linear transform means $L2_i(x)$, wherein the linear transform means $L1_i(x)$, the nonlinear transform means with the masked fixed table $S_i[x]$ and the linear transform means $L2_i(x)$ operate in that round; and

a selector for selecting one of said plurality of nonlinear transform means.

17. (Cancelled)

18. (Currently amended) The encryption device according to claim ~~17~~16, wherein

the fixed tables of said respective nonlinear transform means in said respective encrypting rounds are identical.

19. (Original) The encryption device according to claim 16, wherein

a mask is canceled over subsequent ones of said plurality of encrypting rounds.

20. (Original) The encryption device according to claim 16, wherein

masking is performed in each of a second plurality of encrypting rounds of said first plurality of encrypting rounds, said second plurality being smaller than said first plurality.

21. (Currently amended) An encryption device comprising a random number generator~~means~~ for generating a random ~~number, and a~~number h, where h is an integer between zero and q-1, and a first plurality of encrypting rounds, wherein

i-th one ~~each~~ of said plurality of encrypting rounds comprises nonlinear transform means for nonlinearly transforming an input thereto for that round, where i is an integer; and

~~thereto; and~~ XOR means for XORing a first input thereto and a second input thereto;

the second input to said XOR means is coupled ~~connected~~ to an output of said nonlinear

transform means; and

said nonlinear transform means comprises; ~~therein nonlinear transform means for nonlinearly transforming an input thereto in accordance with a fixed table and in accordance with the random number~~

q sets of fixed values, where q is equal to two, wherein equations, $FM_{i,h} = C_h$ XOR $L1_i(L2_{i-1}(Dh))$ for $i \geq 1$, $C_h = c_{h,15}c_{h,14}...c_{h,0}$, and $D_h = d_{h,15}d_{h,14}...d_{h,0}$, are satisfied, where $FM_{i,h}$ is the i-th fixed value of the h-th set of said q sets of fixed values, where j is an integer,

q sets of fixed values, wherein equations, $(c_{0,j}$ XOR $c_{1,j}) = (0101...01)2$ or $(1010...10)2$ and $(d_{0,j}$ XOR $d_{1,j}) = (0101...01)2$ or $(1010...10)2$ are satisfied, a fixed table before masking is defined as S[x] and i-th masked fixed table is defined as $S_i[x$ XOR $c_{i,j}]$ XOR $d_{i,j}$ for the j-th fixed value;

a selector for selecting one of said q sets of fixed values in response to the random number h;

further XOR means for XORing an input thereto with an XOR of a key with said selected fixed value;

linear transform means $L1_i(x)$,

a plurality of nonlinear transform means for nonlinearly transforming an input in accordance with a fixed table;

linear transform means $L2_i(x)$, wherein the linear transform means $L1_i(x)$, the nonlinear transform means with the masked fixed table $S_i[x]$ and the linear transform means $L2_i(x)$ operate in that round; and

a selector for selecting one of said plurality of nonlinear transform means.

22-24 (Cancelled)

25. (Currently amended) A program stored on a storage medium for use in an encryption device, said program operable to effect the steps of:

selecting one of q sets of fixed values, where q is ~~an integer,~~ equal to two, in response to a random number h, where h is an integer between zero and q-1;

XORing an input value with an XOR of a key with said selected fixed ~~value;~~

value in i-th one of rounds, wherein equations, $FM_{0,h} = C_h$ XOR $L1_0$ (FMin), $C_h = c_{h,15}c_{h,1}...c_{h,0}$, and $D_h = d_{h,15}d_{h,14}...d_{h,0}$, are satisfied, where $FM_{j,h}$ is the i-th fixed value of the h-th set of said q sets of fixed values, where i is an integer and j is an integer;

selecting one set $S_i[x]$ of q sets of masked fixed tables in response to the random

~~number; and~~

number h in that round, wherein equations, $(c_{0,j}$ XOR $c_{1,j}) = (0101...01)2$ or $(1010...10)2$ and $(d_{0,j}$ XOR $d_{1,j}) = (0101...01)2$ or $(1010...10)2$ are satisfied, a fixed table before masking is defined as S[x], and i-th masked fixed table is defined as $S_j[x$ XOR $c_{i,j}]$ XOR $d_{i,j}$ for the j-th fixed value;

nonlinearly transforming an input value in accordance with said selected set ~~of fixed tables.~~$S_j[x]$ of fixed tables in that round; and

linearly transforming the nonlinearly transformed value in that round.

26-28. (Cancelled)

29. (New) The encryption device according to claim 1, characterized in that the linear transform means $L1_i(x)$ is defined as $L1_i(x) = x$.

30. (New) The encryption device according to claim 1, characterized in that the linear transform means $L2_i(x)$ is defined as $L2_i(x) = MixedColumn(Shift(x))$.

31. (New) The encryption device according to claim 1, characterized in that the linear transform means $L2_i(x)$ is defined as Shift(x).

32. (New) The encryption device according to claim 4, characterized in that the linear transform means $L1_i(x)$ is defined as $L1_i(x) = x$.

33. (New) The encryption device according to claim 4, characterized in that the linear transform means $L2_i(x)$ is defined as $L2_i(x) = MixedColumn(Shift(x))$.

34. (New) The encryption device according to claim 4, characterized in that the linear transform means $L2_i(x)$ is defined as Shift(x)

35. (New) The encryption device according to claim 8, characterized in that the linear transform means $L1_i(x)$ is defined as $L1_i(x) = x$.

36. (New) The encryption device according to claim 8, characterized in that the linear transform means $L2_i(x)$ is defined as $L2_i(x) = MixedColumn(Shift(x))$.

37. (New) The encryption device according to claim 8, characterized in that the linear transform means $L2_i(x)$ is defined as Shift(x)

38. (New) An encryption device comprising XOR means and nonlinear transform means, said encryption device further comprising:

a random number generator for generating a random number h, where h is an integer between zero and q-1;

q sets of fixed values, where q is an integer three or more, wherein equations, $FM_{i,h} = C_{\underline{h}}$ XOR L1i(L2i-1(Dh)) for $i \geq 1$, $C_{\underline{h}} = c_{h,15}c_{h,14}...c_{h,0}$, and $D_{\underline{h}} = d_{h,15}d_{h,14}...d_{h,0}$, are satisfied, where i is an integer and j is an integer,

q sets of fixed values, where equations, $(c_{0,j}$ XOR $c_{1,j}) \vee (c_{1,j}$ XOR $c_{2,j}) \vee ... \vee (cq_{-2,j}$ XOR $cq_{-1,j}) = (1111...11)2$ and $(d_{0,j}$ XOR $d_{1,j}) \vee (d_{1,j}$ XOR $d_{2,j}) \vee ... \vee (dq_{-2,j}$ XOR $dq_{-1,j}) = (1111...11)2$, are satisfied, and a fixed table before masking is defined as S[x] and an i-th masked fixed table is defined as S_j[x XOR ch,j] XOR dh,j for the j-th fixed value;

linear transform means $L1_i(x)$ and linear transform means $L2_i(x)$, wherein the linear transform means $L1_i(x)$, the nonlinear transform means with the masked fixed table S_j [x] and the linear transform means $L2_i(x)$ operate in i-th one of rounds; and

a first selector for selecting one fixed value of the h-th set of said q sets of fixed values in response to the random number h;

said XOR means XORing an input thereto with an XOR of a key with said selected fixed value.

39. (New) The encryption device according to claim 38, characterized in that the linear transform means $L1_i(x)$ is defined as $L1_i(x) = x$.

40. (New) The encryption device according to claim 38, characterized in that the linear transform means $L2_i(x)$ is defined as $L2_i(x)$ = MixedColumn(Shift(x)).

41. (New) The encryption device according to claim 38, characterized in that the linear transform means $L2_i(x)$ is defined as Shift(x).

42. (New) An encryption device comprising XOR means and nonlinear transform means, said encryption device further comprising:

a random number generator for generating a random number h, where h is an integer between zero and q-1;

q sets of masked fixed values and q sets of fixed tables, where q is equal to two, wherein equations, $FM_{0,h} = C_h$ XOR $L1_0$ (FMin), $C_h = c_{h,15}c_{h,1}...c_{h,0}$, and $D_h = d_{h,15}d_{h,14}...d_{h,0}$, are satisfied, where $FM_{i,h}$ is the i-th fixed value of the h-th set of said q sets of fixed values, where i is an integer and j is an integer,

q sets of fixed values, wherein equations, ($c_{0,j}$ XOR $c_{1,j}$) = (0101...01)2 or (1010...10)2 and ($d_{0,j}$ XOR $d_{1,j}$) = (0101...01)2 or (1010...10)2 are satisfied, a fixed table before masking is defined as S[x], and i-th masked fixed table is defined as $S_j[x \text{ XOR } c_{i,j}] \text{ XOR } d_{i,j}$ for the j-th fixed value;

a selector for selecting one of said q sets of fixed tables in response to the random number h,

said nonlinear transform means nonlinearly transforming an input thereto in accordance with said selected set of fixed tables; and

a plurality of encrypting rounds, wherein i-th one of said plurality of encrypting rounds comprises the XOR means, the fixed tables, the selector, linear transform means $L1_i(x)$ and linear transform means $L2_i(x)$, for that round, and wherein the fixed tables for said plurality of respective encrypting rounds are identical, and wherein the linear transform means $L1_i(x)$, the nonlinear transform means with the masked fixed table $S_j[x]$ and the linear transform means $L2_i(x)$ operate in that round.

43. (New) The encryption device according to claim 42, characterized in that the linear transform means $L1_i(x)$ is defined as $L1_i(x) = x$.

44. (New) The encryption device according to claim 42, characterized in that the linear transform means $L2_i(x)$ is defined as $L2_i(x)$ = MixedColumn(Shift(x)).

45. (New) The encryption device according to claim 42, characterized in that the linear transform means $L2_i(x)$ is defined as Shift(x).

46. (New) An encryption device comprising XOR means and nonlinear transform means, said encryption device further comprising:

a random number generator for generating a random number h, where h is an integer between zero and q-1;

q sets of masked fixed values and q sets of fixed tables, where q is equal to two, wherein equations, $FM_{i,h} = C_h$XOR L1i(L2i-1(Dh)) for i≥1, $C_h = c_{h,15}c_{h,14}...c_{h,0}$, and $D_h = d_{h,15}d_{h,14}...d_{h,0}$, are satisfied, where $FM_{i,h}$ is the i-th fixed value of the h-th set of said q sets of fixed values, where i is an integer and j is an integer,

q sets of fixed values, wherein equations, $(c_{0,j}$ XOR $c_{1,j}) = (0101...01)2$ or $(1010...10)2$ and $(d_{0,j}$ XOR $d_{1,j}) = (0101...01)2$ or $(1010...10)2$ are satisfied, a fixed table before masking is defined as S[x], and i-th masked fixed table is defined as $S_j[x$ XOR $c_{i,j}]$ XOR $d_{i,j}$ for the j-th fixed value;

a selector for selecting one of said q sets of fixed tables in response to the random number h,

said nonlinear transform means nonlinearly transforming an input thereto in accordance with said selected set of fixed tables; and

a plurality of encrypting rounds, wherein i-th one of said plurality of encrypting rounds comprises the XOR means, the fixed tables, the selector, linear transform means $L1_i(x)$ and linear transform means $L2_i(x)$, for that round, and wherein the fixed tables for said plurality of respective encrypting rounds are identical, and wherein the linear transform means $L1_i(x)$, the nonlinear transform means with the masked fixed table $S_j[x]$ and the linear transform means $L2_i(x)$ operate in that round.

47. (New) The encryption device according to claim 46, characterized in that the linear transform means $L1_i(x)$ is defined as $L1_i(x) = x$.

48. (New) The encryption device according to claim 46, characterized in that the linear transform means $L2_i(x)$ is defined as $L2_i(x)$ = MixedColumn(Shift(x)).

49. (New) The encryption device according to claim 46, characterized in that the linear transform means $L2_i(x)$ is defined as Shift(x).

50. (New) An encryption device comprising XOR means and nonlinear transform means, said encryption device further comprising:

a random number generator for generating a random number h, where h is an integer between zero and q-1;

q sets of masked fixed values and q sets of fixed tables, where q is an integer equal to three or more, wherein equations, $FM_{0,h} = C_h$XOR $L1_0$ (FMin), $C_h = c_{h,15}c_{h,1}...c_{h,0}$, and $D_h = d$

$_{h,15}d_{h,14}...d_{h,0}$, are satisfied, where $FM_{i,h}$ is the i-th fixed value of the h-th set of said q sets of fixed values, where i is an integer and j is an integer,

q sets of fixed values, wherein equations, $(c_{0,j}$ XOR $c_{1,j}) \vee (c_{1,j}$ XOR $c_{2,j}) \vee ... \vee (cq_{-2,j}$ XOR $cq_{-1,j}) = (111...11)2$ and $(d_{0,j}$ XOR $d_{1,j}) \vee (d_{1,j}$ XOR $d_{2,j}) \vee ... \vee (dq_{-2,j}$ XOR $dq_{-1,j}) = (111...11)2$ are satisfied, a fixed table before masking is defined as S[x], and i-th masked fixed table is defined as $S_j[x$ XOR $c_{i,j}]$ XOR $d_{i,j}$ for the j-th fixed value;

a selector for selecting one of said q sets of fixed tables in response to the random number h,

said nonlinear transform means nonlinearly transforming an input thereto in accordance with said selected set of fixed tables; and

a plurality of encrypting rounds, wherein i-th one of said plurality of encrypting rounds comprises the XOR means, the fixed tables, the selector, linear transform means $L1_i(x)$ and linear transform means $L2_i(x)$, for that round, and wherein the fixed tables for said plurality of respective encrypting rounds are identical, and wherein the linear transform means $L1_i(x)$, the nonlinear transform means with the masked fixed table $S_j[x]$ and the linear transform means $L2_i(x)$ operate in that round.

51. (New) The encryption device according to claim 50, characterized in that the linear transform means $L1_i(x)$ is defined as $L1_i(x) = x$.

52. (New) The encryption device according to claim 50, characterized in that the linear transform means $L2_i(x)$ is defined as $L2_i(x)$ = MixedColumn(Shift(x)).

53. (New) The encryption device according to claim 50, characterized in that the linear transform means $L2_i(x)$ is defined as Shift(x).

54. (New) An encryption device comprising XOR means and nonlinear transform means, said encryption device further comprising:

a random number generator for generating a random number h, where h is an integer between zero and q-1;

q sets of masked fixed values and q sets of fixed tables, where q is an integer equal to three or more, wherein equations, $FM_{i,h} = C_{\underline{h}}$ XOR L1i(L2i-1(Dh)) for i≥1, $C_{\underline{h}} = c_{h,15}c_{h,14}...c_{h,0}$, and $D_{\underline{h}} = d_{h,15}d_{h,14}...d_{h,0}$, are satisfied, where $FM_{i,h}$ is the i-th fixed value of the h-th set of said q sets of fixed values, where i is an integer and j is an integer,

q sets of fixed values, wherein equations, $(c_{0,j}$ XOR $c_{1,j}) \vee (c_{1,j}$ XOR $c_{2,j}) \vee ... \vee (cq_{-2,j}$ XOR $cq_{-1,j}) = (111...11)2$ and $(d_{0,j}$ XOR $d_{1,j}) \vee (d_{1,j}$ XOR $d_{2,j}) \vee ... \vee (dq_{-2,j}$ XOR $dq_{-1,j}) = (111...11)2$ are satisfied, a fixed table before masking is defined as S[x], and i-th masked fixed table is defined as $S_j[x$ XOR $c_{i,j}]$ XOR $d_{i,j}$ for the j-th fixed value;

a selector for selecting one of said q sets of fixed tables in response to the random number h,

said nonlinear transform means nonlinearly transforming an input thereto in accordance with said selected set of fixed tables; and

a plurality of encrypting rounds, wherein i-th one of said plurality of encrypting rounds comprises the XOR means, the fixed tables, the selector, linear transform means $L1_i(x)$ and linear transform means $L2_i(x)$, for that round, and wherein the fixed tables for said plurality of respective encrypting rounds are identical, and wherein the linear transform means $L1_i(x)$, the nonlinear transform means with the masked fixed table S_j [x] and the linear transform means $L2_i(x)$ operate in that round.

55. (New) The encryption device according to claim 54, characterized in that the linear transform means $L1_i(x)$ is defined as $L1_i(x) = x$.

56. (New) The encryption device according to claim 54, characterized in that the linear transform means $L2_i(x)$ is defined as $L2_i(x)$ = MixedColumn(Shift(x)).

57. (New) The encryption device according to claim 54, characterized in that the linear transform means $L2_i(x)$ is defined as Shift(x).

58. (New) The encryption device according to claim 16, characterized in that the linear transform means $L1_i(x)$ is defined as $L1_i(x) = x$.

59. (New) The encryption device according to claim 16, characterized in that the linear transform means $L2_i(x)$ is defined as $L2_i(x)$ = MixedColumn(Shift(x)).

60. (New) The encryption device according to claim 16, characterized in that the linear transform means $L2_i(x)$ is defined as Shift(x).

61. (New) The encryption device according to claim 21, characterized in that the linear

transform means $L1_i(x)$ is defined as $L1_i(x) = x$.

62. (New) The encryption device according to claim 21, characterized in that the linear transform means $L2_i(x)$ is defined as $L2_i(x) = MixedColumn(Shift(x))$.

63. (New) The encryption device according to claim 21, characterized in that the linear transform means $L2_i(x)$ is defined as $Shift(x)$.

64. (New) An encryption device comprising a random number generator for generating a random number h, where h is an integer between zero and q-1, and a first plurality of encrypting rounds, wherein

i-th one of said plurality of encrypting rounds comprises nonlinear transform means for nonlinearly transforming an input thereto, and XOR means for XORing a first input thereto with a second input thereto for that round, where i is an integer;

the second input to said XOR means is coupled to an output of said nonlinear transform means; and

said nonlinear transform means comprises:

q sets of fixed values, where q is an integer equal to three or more, wherein equations, $FM_{0,h} = C_{\underline{h}}$ XOR $L1_0$ (FMin), $C_{\underline{h}} = c_{h,15}c_{h,1}...c_{h,0}$, and $D_{\underline{h}} = d_{h,15}d_{h,14}...d_{h,0}$, are satisfied, where $FM_{i,h}$ is the i-th fixed value of the h-th set of said q sets of fixed values, where j is an integer,

q sets of fixed values, wherein equations, $(c_{0,j}$ XOR $c_{1,j}) \vee (c_{1,j}$ XOR $c_{2,j}) \vee ... \vee (cq_{-2,j}$ XOR $cq_{-1,j}) = (111...11)2$ and $(d_{0,j}$ XOR $d_{1,j}) \vee (d_{1,j}$ XOR $d_{2,j}) \vee ... \vee (dq_{-2,j}$ XOR $dq_{-1,j}) = (111...11)2$ are satisfied, a fixed table before masking is defined as S[x], and i-th masked fixed table is defined as $S_j[x$ XOR $c_{i,j}]$ XOR $d_{i,j}$ for the j-th fixed value;

a selector for selecting one of said q sets of fixed values in response to the random number h;

further XOR means for XORing an input thereto with an XOR of a key with said selected fixed value;

linear transform means $L1_i(x)$;

a plurality of nonlinear transform means for nonlinearly transforming an input in accordance with a fixed table;

linear transform means $L2_i(x)$, wherein the linear transform means $L1_i(x)$, the nonlinear transform means with the masked fixed table $S_j[x]$ and the linear transform means $L2_i(x)$ operate in that round; and

a selector for selecting one of said plurality of nonlinear transform means.

65. (New) The encryption device according to claim 64, characterized in that the linear transform means $L1_i(x)$ is defined as $L1_i(x) = x$.

66. (New) The encryption device according to claim 64, characterized in that the linear transform means $L2_i(x)$ is defined as $L2_i(x) = \text{MixedColumn}(\text{Shift}(x))$.

67. (New) The encryption device according to claim 64, characterized in that the linear transform means $L2_i(x)$ is defined as $\text{Shift}(x)$.

68. (New) An encryption device comprising a random number generator for generating a random number h, where h is an integer between zero and q-1, and a first plurality of encrypting rounds, wherein

i-th one of said plurality of encrypting rounds comprises nonlinear transform means for nonlinearly transforming an input thereto, and XOR means for XORing a first input thereto with a second input thereto for that round, where i is an integer;

the second input to said XOR means is coupled to an output of said nonlinear transform means; and

said nonlinear transform means comprises:

q sets of fixed values, where q is an integer equal to three or more, wherein equations, $FM_{i,h} = C_{\underline{h}}$ XOR $L1i(L2i\text{-}1(D_h))$ for $i \geq 1$, $C_h = c_{h,15}c_{h,14}\ldots c_{h,0}$, and $D_h = d_{h,15}d_{h,14}\ldots d_{h,0}$, are satisfied, where $FM_{i,h}$ is the i-th fixed value of the h-th set of said q sets of fixed values, where j is an integer,

q sets of fixed values, wherein equations, $(c_{0,j}$ XOR $c_{1,j}) \vee (c_{1,j}$ XOR $c_{2,j}) \vee \ldots \vee (cq\text{-}_{2,j}$ XOR $cq\text{-}_{1,j}) = (111\ldots11)2$ and $(d_{0,j}$ XOR $d_{1,j}) \vee (d_{1,j}$ XOR $d_{2,j}) \vee \ldots \vee (dq\text{-}_{2,j}$ XOR $dq\text{-}_{1,j}) = (111\ldots11)2$ are satisfied, a fixed table before masking is defined as S[x], and i-th masked fixed table is defined as $S_j[x$ XOR $c_{i,j}]$ XOR $d_{i,j}$ for the j-th fixed value;

a selector for selecting one of said q sets of fixed values in response to the random number h;

further XOR means for XORing an input thereto with an XOR of a key with said selected fixed value;

linear transform means $L1_i(x)$;

a plurality of nonlinear transform means for nonlinearly transforming an input in

accordance with a fixed table;

linear transform means $L2_i(x)$, wherein the linear transform means $L1_i(x)$, the nonlinear transform means with the masked fixed table S_j [x] and the linear transform means $L2_i(x)$ operate in that round; and

a selector for selecting one of said plurality of nonlinear transform means.

69. (New) The encryption device according to claim 68, characterized in that the linear transform means $L1_i(x)$ is defined as $L1_i(x) = x$.

70. (New) The encryption device according to claim 68, characterized in that the linear transform means $L2_i(x)$ is defined as $L2_i(x)$ = MixedColumn(Shift(x)).

71. (New) The encryption device according to claim 68, characterized in that the linear transform means $L2_i(x)$ is defined as Shift(x).

72. (New) A program stored on a storage medium for use in an encryption device, said program operable to effect the steps of:

selecting one set of q sets of fixed values, where q is an integer equal to three or more, in response to a random number h, where h is an integer between zero and q-1;

XORing an input value with an XOR of a key with said selected fixed value in i-th one of rounds, wherein equations, $FM_{0,h} = C_h$ XOR $L1_0$ (FMin), $C_h = c_{h,15}c_{h,1}\ldots c_{h,0}$, and $D_h = d_{h,15}d_{h,14}\ldots d_{h,0}$, are satisfied, where $FM_{i,h}$ is the i-th fixed value of the h-th set of said q sets of fixed values, where i is an integer and j is an integer;

selecting one set S_j [x] of q sets of masked fixed tables in response to the random number h in that round, wherein equations, $(c_{0,j}$ XOR $c_{1,j}) \vee (c_{1,j}$ XOR $c_{2,j}) \vee\ldots\vee (cq_{-2,j}$ XOR $cq_{-1,j})$ = (111...11)2 and $(d_{0,j}$ XOR $d_{1,j}) \vee (d_{1,j}$ XOR $d_{2,j}) \vee\ldots\vee (dq_{-2,j}$ XOR $dq_{-1,j})$ = (111...11)2 are satisfied, a fixed table before masking is defined as S[x], and i-th masked fixed table is defined as Sj[x XOR $c_{i,j}$] XOR $d_{i,j}$ for the j-th fixed value;

nonlinearly transforming an input value in accordance with said selected set S_j [x] of fixed tables in that round; and

linearly transforming an input value and the nonlinearly transformed value in that round.